



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,864	03/05/2002	Sjoblom Hans	150-044	8299
7590	12/13/2005		EXAMINER	
Steven S. Payne 8027 Iliff Drive Dunn Loring, VA 22027			HENEGHAN, MATTHEW E	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/087,864	Applicant(s) HANS, SJOBLOM	
	Examiner Matthew Heneghan	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 March 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 11-14 and 16-20 is/are allowed.
- 6) ☒ Claim(s) 1-10 and 21-32 is/are rejected.
- 7) ☒ Claim(s) 15 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 March 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2/28/03</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-32 have been examined.

Information Disclosure Statement

2. The following Information Disclosure Statement in the instant application has been fully considered:

IDS filed 28 February 2003.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: item "114" in figure 1.
4. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37

Art Unit: 2134

CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

5. Claims 5, 15, and 25 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claims, or amend the claims to place the claims in proper dependent form, or rewrite the claims in independent form. Each claim adds the limitation that the public and private keys are asymmetric; however, since all public/private keys are inherently asymmetric, these dependent claims do not further limit their parent claims; for purposes of the prior art search, each claim stands or falls with its base claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2134

6. Claims 1-6, 9, and 10 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 4,575,621 to Dreifus.

Claim 1 reads: A method for controlling the use of data on a device by a user, comprising the steps of:
issuing a smart card to the user by a first party,
wherein a private key which is assigned to the user is stored on the smart card,
wherein the private key is usable but not known by the user and the private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card;
encrypting data to be sent to the user using a public key assigned to the user before distributing the data to the user; and
after distribution of the data to the user, prompting the user to enter a private key each time the user wants to use the data,
wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the private key.

Claim 5 reads:

The method according to claim 1, wherein the public and private keys are asymmetric public and private keys.

As per claims 1 and 5, Dreifus discloses a system wherein a smart card is disclosed that correlates a card with a user to whom it has been issued by way of a user identifier, and allows transactions after it is determined that the card's identifiers are valid (see column 10, line 13-23). Other user authentication information may be required before the card can be used (see column 17, lines 32-51). Private keys (from public/private key pairs) are used to decrypt messages (see column 13, lines 25-28), and the key is stored and used solely on the card (see column 16, lines 3-6). No mechanism is disclosed for the user to view the private keys, and no reason is suggested for a user to do so. A direct card-to-card key transfer is disclosed (see

Art Unit: 2134

column 16), but this does not require the user to be directly exposed to the key information. The authentication may be executed using the device's display (see column 17, lines 54-56), which inherently requires a prompting whenever the card is to be used.

Claim 2 reads:

The method according to claim 1, wherein the smart card is a credit card.

As per claim 2, the card may be a credit card (see column 7, lines 10-12).

Claim 3 reads:

The method according to claim 1, wherein the smart card is an identification card.

As per claim 3, the card may be used for identification (see column 18, lines 25-49).

Claim 4 reads:

The method according to claim 1, wherein the data is digital information comprises one of computer software, music, literature, audio and/or video information.

As per claim 4, a computer program (i.e. software) may be downloaded that modifies the card's operations (see column 9, lines 37-57).

Claim 6 reads:

The method according to claim 5, wherein the asymmetric public key for the user is obtained from the user.

As per claim 6, keys may be obtained from the terminal (i.e. the user) (see column 9, lines 30-33).

Art Unit: 2134

Claim 9 reads:

The method according to claim 1, wherein the user authenticates the smart card by entering a biometric identification code.

As per claim 9, biometric characteristics such as hand structure retinal patterns, or fingerprints may be used for access (see column 17, lines 46-48).

Claim 10 reads:

The method according to claim 1, wherein a processor in the smart card decrypts the encrypted data using the private key.

As per claim 10, the all encryption/decryption functionality is performed by the card's CPU (see column 8, lines 56-57).

7. Claims 21, 24, 25, and 30-32 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,673,316 to Auerbach et al.

Claim 21 reads:

A method for controlling the use of data on a device by a user, comprising the steps of: encrypting data to be sent to the user using at least one public key assigned to the user before distributing the data to the user; and after distribution of the data to the user, prompting the user to enter at least one private key each time the user wants to use the data, wherein the at least one private key is stored on a smart and the at least one private key is usable but not known by the user and the at least one private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the private key.

Claim 25 reads:

Art Unit: 2134

The method according to claim 21, wherein the at least one public and private keys are asymmetric public and private keys.

Claim 31 reads:

The method according to claim 21, wherein a processor in the smart card decrypts the encrypted data using the private key.

Claim 32 reads:

A method for controlling the use of data on a device by a user, comprising the steps of: encrypting data to be sold to the user by a seller using at least one public key assigned to the user before distributing the data to the user; and after distribution of the data to the user, the user is prompted by the device to enter at least one private key each time the user wants to use the data, wherein the at least one private key is stored on a smart and the at least one private key is usable but not known by the user and the at least one private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the private key.

As per claims 21, 25, 31, and 32, Auerbach discloses a distribution system using a DFWM, which may be embodied as a smart card (see column 7, lines 43-45) that is issued to a user after a registration process (see column 6, line 63 to column 7, line 18). A private key may be assigned to the user for storage on the DFWM for authentication with trusted third parties (see column 7, lines 31-41) that is secret, inaccessible information (unknowable to the user). A purchase transaction takes place in which information is placed within a cryptographic envelope that is encrypted with the DFWM public key (see column 10, lines 6-34). Decryption takes place on the DFWM (see column 10, lines 57-64). The user is prompted for a password for authentication purposes, which triggers a private key lookup (see column 8, lines 15-25 and column 9, lines 6-8).

Art Unit: 2134

Claim 24 reads:

The method according to claim 21, wherein the data is digital information comprises one of computer software, music, literature, audio and/or video information.

As per claim 24, the purchased document may be an MPEG audio/video stream
(see column 4, lines 11-12).

Claim 30 reads:

The method according to claim 21, wherein the user knows all of the private keys except for one private key.

Regarding claim 30, the user doesn't know the one private keys, and there are no other keys to know.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2134

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 4,575,621 to Dreifus as applied to claim 5 above, and further in view of U.S.

Patent No. 4,944,007 to Austin.

Claim 7 reads:

The method according to claim 5, wherein the asymmetric public key for the user is obtained from a public database.

Dreifus does not disclose the source of a card's original keys.

Austin discloses the embedding of the secret key by a credit card issuer (see column 3, lines 9-12), as this allows for a card to be able to prove its authenticity to the association (see column 3, lines 18-22).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further implement the smart card of Dreifus by having a card issuer embed the keys, as disclosed by Austin, as this allows for a card to be able to prove its authenticity to the association.

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 4,575,621 to Dreifus.

Claim 8 reads:

The method according to claim 1, wherein the user authenticates the smart card by entering a personal identification number code.

Dreifus discloses that a user identification code may be required for access (see column 17, lines 52-54), but does not specify that it be a number code.

Official notice is given that it is well-known in the art to implement identification codes or passwords as numbers, so that users may enter the codes using number pads.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dreifus by using number codes for the user identification codes, as is well-known in the art, so that users may enter the codes using number pads.

10. Claims 22, 23, 26, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,673,316 to Auerbach et al. as applied to claims 21 and 25 above, and further in view of U.S. Patent No. 4,575,621 to Dreifus.

Claim 22 reads:

The method according to claim 21, wherein the smart card is a credit card.

Claim 23 reads:

The method according to claim 21, wherein the smart card is an identification card.

Claim 29 reads:

The method according to claim 21, wherein the user authenticates the smart card by entering a biometric identification code.

Regarding claims 22, 23, and 29, Auerbach does not give details about the type of smart card used, or whether it can be used with biometrics.

Dreifus discloses a smart card that is an identification and/or credit card with biometric authentication, as described above, as further suggests that these cards are being used to effect a transaction (see column 1, lines 15-18) and that improper use of

transactions systems can result in serious breaches of high-security systems (see column 2, lines 13-16).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the smart card of Auerbach as an identification or credit card with biometric authentication, as disclosed by Dreifus, in order to effect a transaction that is less likely to result in serious breaches of high-security systems.

Claim 26 reads:

The method according to claim 25, wherein the at least one asymmetric public key for the user is obtained from the user.

Regarding claim 26, Auerbach also does not disclose the original source of a public/private key pair.

Driefus discloses the receiving of keys from a terminal (i.e. the user), as described above, and suggests that this allows for the periodic varying of encryption formats for enhanced security (see column 3, lines 3-6).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further implement the smart card of Auerbach by allowing the entering of keys from the terminal, as disclosed by Dreifus, as this allows for the periodic varying of encryption formats for enhanced security.

11. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,673,316 to Auerbach et al. as applied to claim 25 above, and further in view of U.S. Patent No. 4,944,007 to Austin.

Claim 27 reads:

The method according to claim 25, wherein the at least one asymmetric public key for the user is obtained from a third party.

Auerbach does not disclose the source of a card's original keys.

Austin discloses the embedding of the secret key by a credit card issuer (see column 3, lines 9-12), as this allows for a card to be able to prove its authenticity to the association (see column 3, lines 18-22).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further implement the smart card of Auerbach by having a card issuer embed the keys, as disclosed by Austin, as this allows for a card to be able to prove its authenticity to the association.

12. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,673,316 to Auerbach et al.

Claim 28 reads:

The method according to claim 21, wherein the user authenticates the smart card by entering a personal identification number code.

Auerbach discloses user authentication using passwords, as described above, but does not disclose that the password should be a number code.

Official notice is given that it is well-known in the art to implement identification codes or passwords as numbers, so that users may enter the codes using number pads.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Auerbach by using number codes for passwords, as is well-known in the art, so that users may enter the codes using number pads.

Allowable Subject Matter

Claim 11 reads:

A method for controlling the use of data on a device by a user, comprising the steps of: issuing a smart card to the user by a first party, wherein a first private key which is assigned to the user is stored on the smart card, wherein the first private key is usable but not known by the user and the first private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card; obtaining at least a second set of public and private keys and storing the at least second private key on the smart card; encrypting data to be sent to the user using a first public key assigned to the user and the second public key before distributing the data to the user; and after distribution of the data to the user, prompting the user to enter the first and at least second private keys each time the user wants to use the data, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the first and at least second private keys.

Claim 12 reads:

The method according to claim 11, wherein the smart card is a credit card.

Claim 13 reads:

The method according to claim 11, wherein the smart card is an identification card.

Claim 14 reads:

The method according to claim 11, wherein the data is digital information comprises one of computer software, music, literature, audio and/or video information.

Claim 15 reads:

The method according to claim 11, wherein the public and private keys are asymmetric public and private keys.

Art Unit: 2134

Claim 16 reads:

The method according to claim 15, wherein the asymmetric public keys for the user are obtained from the user.

Claim 17 reads:

The method according to claim 15, wherein the asymmetric public keys for the user are obtained from a public database.

Claim 18 reads:

The method according to claim 11, wherein the user authenticates the smart card by entering a personal identification number code.

Claim 19 reads:

The method according to claim 11, wherein the user authenticates the smart card by entering a biometric identification code.

Claim 20 reads:

The method according to claim 11, wherein a processor in the smart card decrypts the encrypted data using the private key.

13. Claims 11-14 and 16-20 are allowed.

14. Claim 15 would be allowable if rewritten to overcome the objection set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

15. The following is an examiner's statement of reasons for allowance:

Regarding claim 11, no art could be found wherein received data that is doubly encrypted using public keys is decrypted on a smart card using two separate private keys. U.S. Patent No. 5,673,316 to Auerbach et al. discloses the decrypting of doubly encrypted data on a smart card, but one of the encryptions is done using a symmetric

key, and no art could be found that would suggest the use of a public/private key pair in its place. U.S. Patent No. 6,961,858 to Fransdonk discloses a media player that receives a message that is encrypted with two public keys, but one of the decryptions is performed on the player using a player-specific key, rather than on the smartcard.

Claims 12-20 would be allowable based upon their dependence upon claim 11.

16. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH



November 16, 2005

GREGORY MORSE
PATENT EXAMINER
EBC CENTER 2100

